Computation of Darboux polynomials and rational first integrals with bounded degree in polynomial time

Guillaume Chèze

COMPUTATION OF DARBOUX POLYNOMIALS AND RATIONAL FIRST INTEGRALS WITH BOUNDED DEGREE IN POLYNOMIAL TIME

GUILLAUME CHÈZE

Abstract. In this paper we study planar polynomial differential systems of this form:

$$\frac{dX}{dt} = \dot{X} = A(X,Y),\ \frac{dY}{dt} = \dot{Y} = B(X,Y),$$

where $A, B \in \mathbb{Z}[X,Y]$ and $\deg A \leq d$, $\deg B \leq d$, $\|A\|_\infty \leq \mathcal{H}$ and $\|B\|_\infty \leq \mathcal{H}$. A lot of properties of planar polynomial differential systems are related to irreducible Darboux polynomials of the corresponding derivation: $D = A(X,Y)\partial_X + B(X,Y)\partial_Y$. Darboux polynomials are usually computed with the method of undetermined coefficients. With this method we have to solve a polynomial system. We show that this approach can give rise to the computation of an exponential number of reducible Darboux polynomials. Here we show that the Lagutinskii-Pereira's algorithm computes irreducible Darboux polynomials with degree smaller than N, with a polynomial number, relatively to d, $\log(\mathcal{H})$ and N, binary operations. We also give a polynomial-time method to compute, if it exists, a rational first integral with bounded degree.

Introduction

In this paper we study the following planar polynomial differential system:

$$\frac{dX}{dt} = \dot{X} = A(X,Y),\ \frac{dY}{dt} = \dot{Y} = B(X,Y),$$

where $A, B \in \mathbb{Z}[X,Y]$ and $\deg A \leq d$, $\deg B \leq d$, $\|A\|_\infty \leq \mathcal{H}$ and $\|B\|_\infty \leq \mathcal{H}$. We associate to this polynomial differential system the polynomial derivation $D = A(X,Y)\partial_X + B(X,Y)\partial_Y$.

A polynomial f is said to be a *Darboux polynomial*, if $D(f) = g.f$, where g is a polynomial. A lot of properties of a polynomial differential system are related to *irreducible* Darboux polynomials of the corresponding derivation D. Usually Darboux polynomials are computed with the method of undetermined coefficients. In other words, if we suppose that $\deg f \leq N$ then $D(f) = g.f$ gives a polynomial system in the unknown coefficients of g and f. Then we can find f and g if we solve this system. We will see that this strategy can give rise to the computation of an exponential number of reducible Darboux polynomials.
In this paper we show that we can compute all the irreducible Darboux polynomials of degree smaller than N with $\mathcal{O}\Big(\big(dN\log(\mathcal{H})\big)^{\mathcal{O}(1)}\Big)$ binary operations. Our strategy relies on the factorization of the ecstatic curve as suggested by J.V. Pereira in [Per01].
This complexity result implies that, if we use the Prelle-Singer's strategy [PS83],

Date: September 15, 2010.

then we can compute an integrating factor in polynomial-time. With this integrating factor we can then deduce an elementary solution of the given differential equation. We also show that we can decide if D has a rational first integral of degree N. Furthermore, we can compute this rational first integral with $\mathcal{O}\Big(\big(dN\log(\mathcal{H})\big)^{\mathcal{O}(1)}\Big)$ binary operations.

Related results. The computation of a first integral of a polynomial differential system is an old and classical problem. The situation is the following: we want to compute a function $\mathcal{F}$ such that the curves $\mathcal{F}(X,Y)=c$, where c are constants, give orbits of the differential system. Thus we want to find a function $\mathcal{F}$ such that $D(\mathcal{F})=0$.
In 1878, G. Darboux [Dar78] gives a strategy to find first integrals. One of the tool developed by G. Darboux is now called *Darboux polynomials*. There exist a lot of different names in the literature for Darboux polynomials, for example we can find: special integrals, eigenpolynomials, algebraic invariant curves, particular algebraic solutions or special polynomials.

Now recall briefly the history and the use of Darboux polynomials.
G. Darboux shows in [Dar78] that if we have enough Darboux polynomials then there exists a rational first integral for D, i.e. $D(\mathcal{F})=0$ and $\mathcal{F}\in\mathbb{C}(X,Y)$. More precisely, G. Darboux shows that if we have $d(d+1)/2+2$ Darboux polynomials then the derivation has a rational first integral which can be expressed by means of these polynomials. This work is improved by H. Poincaré [Poi91], P. Painlevé [Pai91], and L. Autonne [Aut91] at the end of the XIX century.

Since 1979, a lot of new results appear. In his book [Jou79], J.-P. Jouanolou gives a polynomial derivation with no Darboux polynomials. Then there exist polynomial differential systems with no nontrivial rational first integral.

In [PS83] M. Prelle and M. Singer give a structure theorem for polynomial differential systems with an elementary first integral. Roughly speaking an elementary function is a function which can be written in terms of polynomials, logarithms, exponentials and algebraic extensions. With this structure theorem the authors show how we can compute an elementary first integral if we know all the Darboux polynomials of D.

In [Man93] and [MM97] Y.-K Man and M. MacCallum explain how we can use Prelle-Singer's method in practice. The bottleneck of this method is the computation of Darboux polynomials. Indeed, the method of undetermined coefficients is used. With this method we have to solve a polynomial system, and Y.-K Man in [Man93] explains how to solve this system with a Groebner basis. The resolution of this polynomial system is difficult because no particular structure of this system is known. Furthermore, this polynomial system can give an exponential number of reducible Darboux polynomials.

In [Sin92] M. Singer shows a structure theorem for polynomial differential systems with a Liouvillian first integral. Roughly speaking a Liouvillian function is a function which can be obtained "by quadratures" of elementary functions. C. Christopher in [Chr99] improves this structure theorem, and then he suggests an algorithm to find Liouvillian first integrals.

In a series of papers [DDdMS02, DDdM02a, DDdM02b] the authors describe an algorithm and its implementation for the computation of Liouvillian first integrals. The strategy is in the same spirit as the one proposed by C. Christopher.

Singer's theorem, Christopher's theorem, and Duarte-Duarte-da Mota's algorithm are based on Darboux polynomials.

In [CLP07] the authors define an algebraic, a geometric, an integral, an infinitesimal and an holonomic notion of multiplicity for an irreducible Darboux polynomial. They show that these notions are related. Furthermore, in order to define the algebraic multiplicity they introduce the ecstatic curve and then use some of its properties. We recall the definition and some properties of the ecstatic curve in Section 3. It seems that this curve and some of its properties was already known by M.N. Lagutinskii (1871–1915), see [DLS98], and was rediscovered by J.V. Pereira, see [Per01]. Theorem 2 in [Per01] is the main tool of our algorithms.

In [CMS09, CMS06], the authors give a Las Vegas strategy to decide if there exist Darboux polynomials for a given derivation.

Recently, in [FG10] the authors propose an algorithm to compute a rational first integral without computing Darboux polynomials. Unfortunately, there are no complexity study for this algorithm.

Darboux polynomials are also used in the qualitative study of polynomial system. For example, the inverse integrating factor is a special Darboux polynomial, and, algebraic limit cycles are factors of the inverse integrating factor, see e.g. [GLV96].

We also mention that Darboux polynomials are used in Physics: In [Hew91] the author uses Darboux polynomials in order to find exact solutions to the Einstein field. In [LZ00, Val05, LV08] Darboux polynomials are also used to study the Rikitake system, which is a simple model for the earth's magneto-hydrodynamic.

In [CG03, Gin07] the reader can find some open questions and some relations between the computation of Darboux polynomials and Hilbert's 16th problem.

For other results, references or applications of Darboux polynomials the reader can consult for example [Gor01, DLA06].

Main results. In this paper we show:

Theorem 1. *Let $D = A(X,Y)\partial_X + B(X,Y)\partial_Y$ be a polynomial derivation such that $A(X,Y), B(X,Y) \in \mathbb{Z}[X,Y]$, $\deg A \leq d$, $\deg B \leq d$, $\|A\|_\infty \leq \mathcal{H}$, $\|B\|_\infty \leq \mathcal{H}$ and A, B are coprime.*

1. *We can decide if there exists a finite number of irreducible Darboux polynomials with degree smaller than N in a deterministic way with $\mathcal{O}\Big(\big(dN\log(\mathcal{H})\big)^{\mathcal{O}(1)}\Big)$ binary operations.*
2. *If there exists a finite number of irreducible Darboux polynomials with degree smaller than N then we can compute all of them in a deterministic way with $\mathcal{O}\Big(\big(dN\log(\mathcal{H})\big)^{\mathcal{O}(1)}\Big)$ binary operations.*

To author's knowledge this is the first polynomial-time result on the computation of Darboux polynomials.

In this paper we suppose that A and B have integer coefficients and are coprime. This hypothesis is not restrictive. Indeed, if A and B have rational coefficients then we can always reduce our study to the case of integral coefficients by clearing denominators. Furthermore if A and B have a nontrivial greatest common divisor R then we set $ds = Rdt$. This gives a derivation $D_2 = A/R\partial_X + B/R\partial_Y$. If D_2 has a first integral then D has a first integral, thus the hypothesis "A and B are coprime" is not restrictive.
Furthermore in this paper we describe algorithms in the bivariate case in order to emphasize their role in the Prelle-Singer's algorithm. Nevertheless, Proposition 18 which is our main tool is also true in the multivariate case, i.e. when we consider a derivation $D = A_1\partial_{X_1} + \cdots + A_n\partial_{X_n}$ where $A_i \in \mathbb{Z}[X_1, \ldots, X_n]$. Then the Lagutinskii-Pereira's algorithm, see Section 4, is also correct in the multivariate case.

If the polynomial derivation D has an infinite number of Darboux polynomials then by Darboux's theorem, D has a rational first integral. Thus in this situation the problem is the computation of a rational first integral. We prove the following result:

Theorem 2. *Let $D = A(X,Y)\partial_X + B(X,Y)\partial_Y$ be a polynomial derivation such that $A(X,Y), B(X,Y) \in \mathbb{Z}[X,Y]$, $\deg A \leq d$, $\deg B \leq d$, $\|A\|_\infty \leq \mathcal{H}$, $\|B\|_\infty \leq \mathcal{H}$ and A, B are coprime.*

1. *We can decide if there exists a rational first integral $\mathcal{F}$ of degree smaller than N with $\mathcal{O}\Big(\big(dN\log(\mathcal{H})\big)^{\mathcal{O}(1)}\Big)$ binary operations.*
2. *If there exists a rational first integral with degree smaller than N then we can compute it in a deterministic way with $\mathcal{O}\Big(\big(dN\log(\mathcal{H})\big)^{\mathcal{O}(1)}\Big)$ binary operations.*

To author's knowledge this is the first polynomial-time result on the computation of rational first integrals.

Structure of this paper. In Section 1 we recall some classical results about Darboux polynomials, the spectrum of a rational function and the complexity of bivariate factorization. In Section 2 we show that the method of undetermined coefficients can give an exponential number of reducible Darboux polynomials. In Section 3 we give the definition and some properties of the ecstatic curve. In Section 4 we prove Theorem 1 and in Section 5 we prove Theorem 2. At last in Section 6 we ask two questions about complexity and polynomial differential equations.

Notations. Let $f(X,Y) = \sum_{i,j} f_{i,j}X^iY^j \in \mathbb{Z}[X,Y]$ be a polynomial.
$\|f\|_\infty = max_{i,j}|f_{i,j}|$ is the height of the polynomial f.
$\deg f$ is the total degree of the polynomial f. The degree of a reduced rational function p/q is the maximum of $\deg p$ and $\deg q$.
The bit-size of a bivariate polynomial f is $(\deg f)^2\log(\|f\|_\infty)$.
∂_X (resp. ∂_Y) denotes the derivative relatively to the variable X (resp. Y).
We set: $\operatorname{div}(A,B) = \partial_X A + \partial_Y B$.

1. Classical results

1.1. Darboux polynomials.

Definition 3. Let $D = A(X,Y)\partial_X + B(X,Y)\partial_Y$ be the derivation associated to the planar polynomial differential system

$$\dot{X} = A(X,Y), \quad \dot{Y} = B(X,Y),$$

where $A, B \in \mathbb{Z}[X,Y]$.
A polynomial $f \in \mathbb{C}[X,Y]$ is said to be a Darboux polynomial of D if there exists a polynomial $g \in \mathbb{C}[X,Y]$ such that $D(f) = g.f$.
The polynomial g is called the cofactor of f.
If $\mathcal{F}$ is a function such that $D(\mathcal{F}) = 0$ then we said that $\mathcal{F}$ is a first integral of D.

Proposition 4. *Let f be a polynomial and let $f = f_1 f_2$ be a factorization of f where f_1 and f_2 are coprime. Then f is a Darboux polynomial with cofactor g if and only if f_1 and f_2 are Darboux polynomials with cofactors g_1 and g_2. Furthermore $g = g_1 + g_2$.*

Proof. See for example Lemma 8.3 page 216 in [DLA06]. □

Now we recall Darboux's Theorem.

Theorem 5 (Darboux's Theorem)**.** *Let $A, B \in \mathbb{Z}[X,Y]$ and let $D = A\partial_X + B\partial_Y$. If $f_1, \ldots, f_m \in \mathbb{C}[X,Y]$ are relatively prime irreducible Darboux polynomials for $i = 1, \ldots, m$, then either $m < d(d+1)/2 + 2$ where $d = \max(\deg A, \deg B)$ or there exist integers n_i not all zero such that $D(w) = 0$, where $w = \prod_{i=1}^{m} f_i^{n_i}$. In the latter case, if f is any irreducible Darboux polynomial, then either there exists λ, μ in $\mathbb{C}$, not both zero such that f divides $\lambda \prod_{i\in I} f_i^{n_i} - \mu \prod_{j\in J} f_j^{-n_j}$ where $I = \{i \,|\, n_i \geq 0\}$ and $J = \{j \,|\, n_j < 0\}$, or G divides $\gcd(A,B)$.*

Proof. See [Dar78] or [Sin92]. □

Definition 6. A function R is an integrating factor if

$$D(R) = -\mathrm{div}(A,B)R.$$

Remark 7. We remark that an integrating factor satisfies also one of these equivalent conditions:

$$\mathrm{div}(RA, RB) = 0, \ \partial_X(RA) = -\partial_Y(RB).$$

If we know an integrating factor then we can deduce a first integral. Indeed, if R is an integrating factor then

$$\mathcal{F} = \int RB dX - \int \Big(RA + \partial_Y \int RB dX \Big) dY \tag{1.1}$$

is a first integral.

1.2. Elementary solutions.

The following theorem is due to M. Prelle and M. Singer, see [PS83].

Theorem 8 (Prelle-Singer)**.** *If a polynomial differential system has an elementary first integral then there exists an integrating factor which is a Kth root of a rational function.*

This gives the following method to compute an elementary first integral. This method is called the Prelle-Singer's method. Here we follow the description given in [Man93].

Prelle-Singer's method
Input: $D = A(X,Y)\partial_X + B(X,Y)\partial_Y$ a polynomial derivation, and N an integer.
Output: An elementary first integral, if it exists, constructed with Darboux polynomials of degree smaller than N.

(1) Set $n = 1$.
(2) Find all monic irreducible polynomials f_i such that $\deg f_i \leq n$ and f_i divides $D(f_i)$.
(3) Let $D(f_i) = g_i f_i$. Decide if there are constants n_i, not all zero, such that
$$\sum_{i=1}^{m} n_i g_i = 0.$$
If such n_i exist then $\prod_{i=1}^{m} f_i^{n_i}$ is a first integral.
If no such n_i exist then go to the next step.
(4) Decide if there are constants n_i, such that
$$\sum_{i=1}^{m} n_i g_i = -\mathrm{div}(A,B).$$
If such n_i exist then $\prod_{i=1}^{m} f_i^{n_i}$ is an integrating factor for the given differential equation. A first integral is given by the formula (1.1).
If no such n_i exists then go to the next step.
(5) Increase the value n by 1. If n is greater than N then return failure otherwise repeat the whole procedure.

If we want to compute an integrating factor, it is well known, see [Man93], that step 2 is the most difficult step of the Prelle-Singer's method. Indeed, when we have all the irreducible Darboux polynomials we just have to solve linear systems (see Step 3 and Step 4) to deduce and integrating factor.

Remark 9. In Prelle-Singer's method the user must give a bound N. Nowadays we cannot remove this input. Indeed, we do not know a bound on the maximal degree of irreducible Darboux polynomials of a given derivation. This is an open question and appears in [Poi91, PS83]. The following example shows that we cannot get a bound in term of the degree of D only. The bound must also take into account the coefficients of D.
Example: The derivation $D = (n+1)X\partial_X + nY\partial_Y$ has $X^n - Y^{n+1}$ as Darboux polynomial.

1.3. **Spectrum of a rational function.** In this subsection we recall the definition and a property of the spectrum of a rational function. This notion is used in Section 5.

Definition 10. A rational function $f(X,Y) \in \mathbb{Q}(X,Y)$ is said to be composite if it can be written $f = u \circ h$ where $h(X,Y) \in \mathbb{Q}(X,Y)$ and $u \in \mathbb{Q}(T)$ such that $\deg(u) \geq 2$. Otherwise f is said to be non-composite.

Definition 11. Let $f = p/q \in \mathbb{Q}(X,Y)$ be a reduced rational function of degree d. The set

$$\sigma(p,q) = \{(\lambda:\mu) \in \mathbb{P}^1_{\mathbb{C}} \quad | \quad \lambda p + \mu q \text{ is reducible in } \mathbb{C}[X,Y], \\ \text{or } \deg(\lambda p + \mu q) < d\}$$

is the spectrum of $f = p/q$. We recall that a polynomial reducible in $\mathbb{C}[X,Y]$ is said to be absolutely reducible.

The spectrum $\sigma(p,q)$ is finite if and only if p/q is non-composite and if and only if the pencil of algebraic curves $\lambda p + \mu q = 0$, has an irreducible general element (see for instance [Jou79, Chapitre 2, Théorème 3.4.6] or [Bod08, Theorem 2.2] for detailed proofs).
To author's knowledge, the first effective result on the spectrum has been given by Poincaré [Poi91]. In this paper, Poincaré gives a relation between the number of saddles of a polynomial vector field and the spectrum. He also shows that $|\sigma(p,q)| \leq (2d-1)^2 + 2d + 2$. This bound was improved only recently by Ruppert [Rup86] who proved the following result:

Proposition 12. *If $p/q \in \mathbb{Q}(X,Y)$ is a reduced non-composite rational function of degree d then $|\sigma(p,q)| \leq d^2 - 1$.*

This result was obtained as a byproduct of a very interesting technique developed to decide the reducibility of an algebraic plane curve.
Several papers improve this result, see e.g. [Lor93, Vis93, AHS03, Bod08, BC08].

Remark 13. If p/q is a reduced non-composite rational first integral of D then $p+\lambda q$, where $\lambda \in \mathbb{C}$, are Darboux polynomials. Then D has infinitely many irreducible Darboux polynomials because the spectrum $\sigma(p,q)$ is finite.

1.4. **Complexity results.** In this paper we consider the dense representation of polynomials in the usual monomial basis. We recall that we can factorize in a deterministic way an integer univariate polynomial f with $\mathcal{O}\Big(\big(d\log(\mathcal{H})\big)^{\mathcal{O}(1)}\Big)$ binary operations, where d is the degree of f and $\mathcal{H}$ its height, see e.g. [Sch84]. An algorithm with this kind of complexity is called a polynomial-time algorithm because its complexity is bounded by a polynomial in the size of the input. We recall that the bit-size of an univariate polynomial f of degree d and height $\mathcal{H}$ is $d\log(\mathcal{H})$.
The first polynomial-time algorithm for the factorization of univariate polynomials is due to Lenstra, Lenstra and Lovasz, see [LLL82]. However this algorithm, called LLL, is probabilistic because it uses Berlekamp's algorithm which is probabilistic, see [Ber70]. Nevertheless, there exist deterministic polynomial-time algorithms, see e.g. [Sch84, KLL88]. In [Sch84, KLL88] the strategy is numerical. Instead of computing a modular factorization as in [LLL82], the authors propose to compute a complex root with a sufficiently high precision.

In [Kal85b] the author shows that we can reduce bivariate factorization to univariate factorization. Then we get a deterministic polynomial-time algorithm for the factorization of integer bivariate polynomials. Another polynomial-time algorithm is proposed in [Len84], the authors extend to the multivariate case the LLL algorithm.
Few time later, several papers see [Kal85a, DT89, Tra85], show that we can also

compute the absolute factorization (i.e. the factorization in $\overline{\mathbb{Q}}[X,Y]$, where $\overline{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$) of integer bivariate polynomials with a deterministic polynomial-time algorithm. Thus there exist deterministic algorithms which perform the absolute factorization of a bivariate polynomial $f(X,Y) \in \mathbb{Q}[X,Y]$ of degree d and height $\mathcal{H}$ with $\mathcal{O}\Big(\big(d\log(\mathcal{H})\big)^{\mathcal{O}(1)}\Big)$ binary operations.
For the history of factorization's algorithm the reader can consult [Kal90, Kal92]. For more recent results about complexity and bivariate polynomials factorization see [Gao03, BLS+04, Lec06, BvHKS09, CL07, AKS07, Wei].

We also mention here that we can solve a linear system, and compute a determinant, with coefficients in $\mathbb{Z}$ or in $\mathbb{Z}[X,Y]$, in polynomial-time, see e.g. [Yap00, BCS97, HS75]. This will be useful in our complexity analysis.

2. The method of undetermined coefficients

Usually, Darboux polynomials are computed with the method of undetermined coefficients. In other words, we write: $D(f) = g.f$ with $\deg g \leq d$, where d is the degree of D, and $\deg f \leq N$. This gives a polynomial system in the unknown coefficients of g and f. This system has $\mathcal{O}(N^2+d^2)$ unknowns. In this section, we show that the method of undetermined coefficients can give an exponential numbers of *reducible* Darboux polynomials. We recall that only *irreducible* Darboux polynomials are useful because the product of Darboux polynomials is a Darboux polynomial, see Proposition 4.

Lemma 14. *If we consider the following derivation:*

$$D = (\partial_Y \mathcal{F})\partial_X - (\partial_X \mathcal{F})\partial_Y, \text{ with } \mathcal{F}(X,Y) = Y\prod_{i=1}^{d-1}(X+i) + X,$$

then there are at least $2^{d-1}+1$ *Darboux polynomials with degree smaller than* d.

Proof. In this situation $X+i$, $i=1,\dots,d-1$, are irreducible Darboux polynomials. Thus

$$\prod_I (X+i), \text{ where } I \text{ is a subset of } \{1,\dots,d-1\}$$

is a Darboux polynomial. We have 2^{d-1} such Darboux polynomials and these polynomials have a degree smaller than $d-1$. Furthermore $\mathcal{F}$ is an irreducible Darboux polynomial and $\deg \mathcal{F} = d$. This gives the desired result. □

Remark 15. In Lemma 14, we give a derivation with a rational first integral. It would be interesting to have the same kind of result with a derivation with no rational first integral.

In the situation of Lemma 14, $\mathcal{F}$ is an irreducible Darboux polynomial of degree d. Thus if we want to find all the irreducible Darboux polynomials, then we have to consider polynomials f with degree smaller or equal to d in the polynomial system $D(f) = g.f$. Now, Lemma 14 implies that *we have at least* $2^{d-1}+1$ *solutions for the system* $D(f) = g.f$ *with* $\deg f \leq d$.
Then we can conclude: *in the worst case the method of undetermined coefficients gives an exponential number, in* d*, of reducible Darboux polynomials.*

The problem comes from *reducible* Darboux polynomials. The recombination of irreducible Darboux polynomials gives an exponential number of Darboux polynomials. We can "avoid" this problem. Indeed, we can add to the system $D(f) = g.f$, forms $\varphi_{i,N}(f)$, $i = 1, \ldots, T$, such that $\varphi_{i,N}(f) = 0$, for all $i = 1, \ldots, T$ if and only if f is an absolutely reducible polynomials with degree N. Such forms exist and they are called Noether's forms, see [Rup86, Sch00]. Unfortunately, to author's knowledge, the number T of these forms is exponential in N. More precisely, the number of Noether's forms is equal to $\binom{2N^2-3N+1}{N^2-1}$. With Stirling's formula we can show, when N tends to infinity:

$$T = \binom{2N^2 - 3N + 1}{N^2 - 1} \sim \frac{2^{2N^2-3N+1}}{e^{9/4}\sqrt{\pi}N}.$$

Thus in this case we have an exponential number of equations, and then we get a method with an exponential complexity in N.

We remark that there exists a strategy to compute the leading term of Darboux polynomials, see e.g.[Chr94]. This strategy gives a net gain in practical examples, see [MM97]. However, this strategy do not detect the leading term of an irreducible Darboux polynomial. Then, even if we add this strategy to the method of undetermined coefficient, we still get an exponential number of Darboux polynomials.

The exponential complexity is related to the recombination of irreducible Darboux polynomials. Exponential complexity due to recombinations appears also when we study factorization algorithms. However, we can factorize polynomials in polynomial-time as mentioned in Section 1.4. In the following we show that we can reduce the computation of irreducible Darboux polynomials to the factorization of a bivariate polynomial. Then, we will deduce a polynomial-time algorithm for the computation of irreducible Darboux polynomials.

3. The ecstatic curve

Definition 16. Let D be a polynomial derivation, the Nth ecstatic curve of D, $\mathcal{E}_{\mathcal{B},N}(D)$, is given by the polynomial

$$\det \begin{pmatrix} v_1 & v_2 & \cdots & v_l \\ D(v_1) & D(v_2) & \cdots & D(v_l) \\ \vdots & \vdots & \cdots & \vdots \\ D^{l-1}(v_1) & D^{l-1}(v_2) & \cdots & D^{l-1}(v_l) \end{pmatrix},$$

where $\mathcal{B} = \{v_1, v_2, \ldots, v_l\}$ is a basis of $\mathbb{C}[X, Y]_{\leq N}$, the $\mathbb{C}$-vector space of polynomials in $\mathbb{C}[X, Y]$ of degree at most N, $l = (N+1)(N+2)/2$, and $D^k(v_i) = D\big(D^{k-1}(v_i)\big)$. When $\mathcal{B}$ is the monomial basis, we denote by $\mathcal{E}_N(D)$ the ecstatic curve.

Now, we remark that the ecstatic curve is independent of the chosen basis of $\mathbb{C}[X, Y]_{\leq N}$ up to a multiplicative constant.

Proposition 17. *Let $\mathcal{B}$ be a basis of $\mathbb{C}[X, Y]_{\leq N}$. We have*

$$\mathcal{E}_{\mathcal{B},N}(D) = c.\mathcal{E}_N(D),$$

where $c \in \mathbb{C}^*$.

Proof. We are going to show that $\mathcal{E}_{\mathcal{B},N}(D)$ is the determinant of an endomorphism. Consider

$$\begin{array}{rcl} \mathcal{D} : \mathbb{C}(X,Y)[U,V]_{\leq N} & \longrightarrow & \mathbb{C}(X,Y)[U,V]_{\leq N} \\ U^iV^j & \longmapsto & \displaystyle\sum_{0\leq k+l\leq N} D^{\mathrm{cantor}(k,l)}(X^iY^j)U^kV^l \end{array}$$

where U and V are new independent variables, $\mathbb{C}(X,Y)[U,V]_{\leq N}$ is the $\mathbb{C}(X,Y)$ vector space of polynomials with coefficients in $\mathbb{C}(X,Y)$, and with a degree relatively to U and V at most N. Furthermore cantor is the following map:

$$\begin{array}{rcl} \mathrm{cantor} : \mathbb{N}^2 & \longrightarrow & \mathbb{N} \\ (k,l) & \longmapsto & \dfrac{(k+l)^2+3k+l}{2}. \end{array}$$

This application maps $(0,0)$ to 0, $(0,1)$ to 1, $(1,0)$ to 2, $(0,2)$ to 3... That is to say, the monomials U^kV^l are ordered with a graded lexicographic order.

$\mathcal{D}$ is defined on a basis thus $\mathcal{D}$ is a well defined endomorphism. $\mathcal{E}_N(D)$ is the determinant of this endomorphism written in the monomial basis.

Now we remark that:

$$\mathcal{D}\Big(\sum_{0\leq i+j\leq N} p_{i,j}U^iV^j\Big) = \sum_{0\leq k+l\leq N}\Big(D^{\mathrm{cantor}(k,l)}(\sum_{0\leq i+j\leq N} p_{i,j}X^iY^j)\Big)U^kV^l,$$

where $p_{i,j}\in\mathbb{C}$.
Each element of the basis $\mathcal{B}$ can be written $\sum_{i,j} p_{i,j}X^iY^j$ with $p_{i,j}\in\mathbb{C}$. We can also consider a basis $\mathcal{B}'$ of the $\mathbb{C}(X,Y)$ vector-space $\mathbb{C}(X,Y)[U,V]_{\leq N}$, such that each element is written $\sum_{i,j} p_{i,j}U^iV^j$ with $p_{i,j}\in\mathbb{C}$. Thus $\mathcal{E}_{\mathcal{B},N}(D)$ is the determinant of $\mathcal{D}$ written with $\mathcal{B}'$ in the domain, and with the monomial basis in the target space. As $p_{i,j}\in\mathbb{C}$, this gives the desired result. □

The following proposition is due to J.-V. Pereira, see [Per01, Proposition 1]. It is the key point of our algorithm: it shows that the computation of Darboux polynomials can be reduced to the factorization of $\mathcal{E}_N(D)$. We give a proof in order to ease the readability of the paper.

Proposition 18. *Every Darboux polynomial, relatively to D, of degree smaller than N is a factor of $\mathcal{E}_N(D)$.*

Proof. Let $F\in\mathbb{C}[X,Y]_{\leq N}$ be a Darboux polynomial. By Proposition 17 we can choose a basis $\mathcal{B}$ where $v_1=F$.
Furthermore, we have:

$$\begin{array}{rcl} D(F) & = & g_1F, \\ D^2(F) & = & D(g_1F) = \big(g_1^2+D(g_1)\big)F = g_2F, \\ & \vdots & \\ D^{l-1}(F) & = & g_{l-1}F, \end{array}$$

where g_1, g_2, ..., g_{l-1} are polynomials.
Thus F is a factor of $\mathcal{E}_{\mathcal{B},N}(D)$ and this concludes the proof. □

Remark 19. The converse is false. Indeed, consider the derivation $D=-2X^2\partial_X+(1-4XY)\partial_Y$. Then $\mathcal{E}_1(D)=YX^4$ but Y is not a Darboux polynomial.

We know by Darboux's Theorem, see Theorem 5, that if a derivation has a rational first integral then there are infinitely many irreducible Darboux polynomials. Thus if D has a rational first integral then by Proposition 18, $\mathcal{E}_N(D)$ has infinitely many irreducible factors. This gives $\mathcal{E}_N(D) = 0$, and also $\mathcal{E}_M(D) = 0$ for M bigger than N. The following proposition says that the converse is also true. This proposition will be useful in Section 5 when we will study the computation of rational first integrals.

Proposition 20. *We have $\mathcal{E}_N(D) = 0$ and $\mathcal{E}_{N-1}(D) \neq 0$ if and only if D admits a rational first integral of exact degree N.*

Proof. See [Per01, Theorem 1]. □

In our complexity study we will need to know the bit-size of $\mathcal{E}_N(D)$. We recall that the bit-size of $\mathcal{E}_N(D)$ is: $\big(\deg(\mathcal{E}_N(D))\big)^2 \log\big(\|\mathcal{E}_N(d)\|_\infty\big)$. Thus in the following we are going to compute the degree and the height of $\mathcal{E}_N(D)$.

Proposition 21. *Let $D = A(X,Y)\partial_X + B(X,Y)\partial_Y$ be a polynomial derivation, where $\deg A, \deg B \leq d$. The degree of $\mathcal{E}_N(D)$ is at most $N.l + (d-1).(l-1).l/2$, where $l = (N+1)(N+2)/2$.*

Proof. By definition of a determinant we have:

$$\deg \mathcal{E}_N(D) \leq \sum_{k=0}^{l-1} \deg\big(D^k(v_i)\big),$$

where $D^0(v_i) = v_i$.
A straightforward computation gives $\deg D^k(v_i) \leq k(d-1) + N$. Then

$$\begin{aligned} \deg \mathcal{E}_N(D) &\leq \sum_{k=0}^{l-1} \big(k(d-1) + N\big), \\ &\leq N.l + (d-1)\sum_{k=0}^{l-1} k, \\ &\leq N.l + (d-1).(l-1).l/2. \end{aligned}$$

This gives the desired result. □

Corollary 22. *Under the hypothesis of Proposition 21, we have $\deg \mathcal{E}_N(D)$ belongs to $\mathcal{O}(dN^4)$.*

Proposition 23. *The height $\|\mathcal{E}_N(D)\|_\infty$ satisfies*

$$\|\mathcal{E}_N(D)\|_\infty \leq \Big(2l\mathcal{H}\big(l(d-1)+N\big)^3\Big)^{l(l-1)/2}.$$

Proof. First we recall that if f_1 and f_2 are two polynomials with total degree smaller than d then we have

$$\|f_1.f_2\|_\infty \leq (d+1)^2 \|f_1\|_\infty \|f_2\|_\infty.$$

This gives for $f \in \mathbb{C}[X,Y]_{\leq N}$,

$$\|D(f)\|_\infty \leq 2\mathcal{H}N^3 \|f\|_\infty.$$

By induction, using $(N+k(d-1)+1)^2 \leq (N+k(d-1))^3$, we get

$$\|D^i(f)\|_\infty \leq 2^i\mathcal{H}^i\Big(\prod_{k=0}^{i-1}\big(k(d-1)+N\big)^3\Big)\|f\|_\infty, \text{ where } i \geq 1.$$

By definition of a determinant, we have:

$$\|\mathcal{E}_N(D)\|_\infty \leq \sum_{\sigma\in\mathfrak{S}_l}\prod_{i=0}^{l-1}\|D^i(v_{\sigma(i+1)})\|_\infty,$$

where $\{v_1,\ldots,v_l\}$ is the monomial basis of $\mathbb{C}[X,Y]_{\leq N}$. We get then:

$$\begin{aligned}\|\mathcal{E}_N(D)\|_\infty &\leq l!\prod_{i=1}^{l-1}2^i\mathcal{H}^i\Big(\prod_{k=0}^{i-1}\big(k(d-1)+N\big)^3\Big)\\ &\leq l!\prod_{i=1}^{l-1}2^i\mathcal{H}^i\Big(\big(l(d-1)+N\big)^{3i}\Big)\\ &\leq \Big(2l\mathcal{H}\big(l(d-1)+N\big)^3\Big)^{l(l-1)/2}.\end{aligned}$$

□

Corollary 24. *Under the hypothesis of Proposition 23, the bit-size of $\mathcal{E}_N(D)$ belongs to $\mathcal{O}\Big(\big(dN\log(\mathcal{H})\big)^{\mathcal{O}(1)}\Big)$.*

Proof. By Corollary 22 and Proposition 23 the bit-size of $\mathcal{E}_N(D)$ is bounded by

$$(dN^4)^2.l.(l-1).\log\Big(2l\mathcal{H}\big(l(d-1)+N\big)^3\Big).$$

This gives the desired result. □

4. D has a finite number of irreducible Darboux polynomials

If D has a finite number of irreducible Darboux polynomials then the ecstatic curve $\mathcal{E}_N(D)$ is non-zero by Proposition 20. It follows that we can compute irreducible Darboux polynomials with a bivariate factorization algorithm thanks to Proposition 18. It seems that Proposition 18 has been proved by M.N. Lagutinskii and rediscovered by J.V. Pereira, see [Per01, Theorem 2]. Then we call "Lagutinskii-Pereira's algorithm" the following algorithm.

Lagutinskii-Pereira's algorithm
Input: A polynomial derivation $D = A(X,Y)\partial_X + B(X,Y)\partial_Y$, and N an integer.
Output: The finite set S of all the absolute irreducible Darboux polynomials with degree smaller than N or "There exists an infinite number of irreducible Darboux polynomials".

(1) $S = \{\}$.
(2) Compute $\mathcal{E}_N(D)$.
(3) If $\mathcal{E}_N(D) = 0$ then Return "There exists an infinite number of irreducible Darboux polynomials" else go to step 4, end If.
(4) Compute the set $f_1,\ldots,f_m$ of all absolutely irreducible factors of $\mathcal{E}_N(D)$ with degree smaller than N .

(5) For $i := 1, \dots, m$ do: If $\gcd(f_i, D(f_i)) = f_i$ then add f_i to S, end If, end For.
(6) Return S.

Proposition 25. *The Lagutinskii-Pereira's algorithm is correct.*

Proof. This is a straightforward consequence of Proposition 18. □

Now we can prove Theorem 1.

Proof. The Lagutinskii-Pereira's algorithm is correct and works with the claimed complexity. Indeed, we can compute $\mathcal{E}_N(D)$ in polynomial-time because it is a determinant. Furthermore, by Corollary 24 we know that the bit-size of $\mathcal{E}_N(D)$ belongs to $\mathcal{O}\Big(\big(dN\log(\mathcal{H})\big)^{\mathcal{O}(1)}\Big)$. Then we can compute the absolutely irreducible factors of $\mathcal{E}_N(D)$ with $\mathcal{O}\Big(\big(dN\log(\mathcal{H})\big)^{\mathcal{O}(1)}\Big)$ binary operations, see Section 1.4. As gcd computations can also be performed in polynomial-time we obtain the desired result. □

We also deduce:

Corollary 26. *Under conditions of Theorem 1, if there exists an integrating factor R such that $R = \prod_i f_i^{n_i}$, where f_i are Darboux polynomials with degree smaller than N, then we can compute R with $\mathcal{O}\Big(\big(dN\log(\mathcal{H})\big)^{\mathcal{O}(1)}\Big)$ binary operations.*

Proof. We compute Darboux polynomials with the Lagutinskii-Pereira's algorithm and then we solve a linear system as in Step 4 of the Prelle-Singer's method, see Section 1. □

This corollary implies that we can compute an integrating factor corresponding to an elementary first integral with the Prelle-Singer's method with $\mathcal{O}\Big(\big(dN\log(\mathcal{H})\big)^{\mathcal{O}(1)}\Big)$ binary operations.

5. D has a rational first integral

We have seen in Section 3 that is easy to test if a derivation has a rational first integral with degree smaller than N. Indeed, we just have to compute the ecstatic curve $\mathcal{E}_N(D)$ and check if it is the zero polynomial. In this section, we show how we can compute this rational first integral.

5.1. Computation of a Darboux polynomials with degree N.

In this section we suppose that D has a rational first integral p/q with degree N. Then p and q are Darboux polynomials with degree N. By Proposition 20, $\mathcal{E}_N(D) = 0$. Thus we cannot compute p and q as factors of $\mathcal{E}_N(D)$. The strategy is then the following: compute one Darboux polynomial with degree N, compute its cofactor, and then deduce p and q.
Now we explain how we can compute a Darboux polynomial with degree N.

Definition 27. Let D be a polynomial derivation, $\mathcal{E}_{N,0}(D)$, is the polynomial $\mathcal{E}_{\mathcal{B}^0,N}(D)$ where $\mathcal{B}^0$ is the monomial basis of the $\mathbb{C}$-vector space of polynomials in $\mathbb{C}[X, Y]$ of degree at most N with constant term equal to zero.

We have the following property.

Proposition 28. *Let p/q be a non-composite rational first integral of D, such that* $\deg(p/q) = N$, *and* $p(0,0)q(0,0) \neq 0$.

(1) *We have* $\mathcal{E}_{N,0}(D) \neq 0$ *in* $\mathbb{Q}[X,Y]$.
(2) *If we set* $(\lambda_0, \mu_0) = \big(-q(0,0), p(0,0)\big)$ *then* $\lambda_0 p + \mu_0 q$ *is a factor of* $\mathcal{E}_{N,0}(D)$.

Proof. This proof follows very closely the proof of Theorem 5.3 and Proposition 5.2 in [CLP07].
First, we prove that $\mathcal{E}_{N,0}(D) \neq 0$.
We suppose the converse: $\mathcal{E}_{N,0}(D) = 0$ and we show that it is absurd.
If $\mathcal{E}_{N,0}(D) = 0$ then the columns of the matrix are linearly dependent. Hence there are rational functions $c_i(X,Y) \in \mathbb{Q}(X,Y)$ such that

$$\mathcal{N}_j := \sum_{i=1}^{k} c_i D^j(v_i) = 0,\ j = 0, \dots, k-1 \tag{5.1}$$

with $k = (N+1)(N+2)/2 - 1$. Now, take k to be the smallest value such that for $i = 1, \dots, k$ there exists rational functions c_i, not all zero, and $v_i \in \mathbb{C}[X,Y]_{\leq N,0}$, linearly independent over $\mathbb{Q}$ such that equalities (5.1) holds. It is clear that $k > 1$. We have:

$$D(\mathcal{N}_j) - \mathcal{N}_{j+1} = \sum_{i=1}^{k} D(c_i) D^j(v_i) = 0,\ j = 0, \dots, k-2,$$

and so from the minimality of k, we see that the terms $D(c_i)$ must all vanish. Hence, each of the c_i are either rational first integrals or constants.
Now, we consider the polynomial $G = \lambda p + \mu q$ where $(\lambda : \mu)$ does not belongs to $\sigma(p,q) \cup \{(\lambda_0 : \mu_0)\}$. This choice is possible because by Proposition 12, $\sigma(p,q)$ is finite. Then G is absolutely irreducible, $\deg G = N$ and $G(0,0) \neq 0$. We also remark that c_i are constants for all (x,y) such that $G(x,y) = 0$, because p/q is a first integral. We denote by $c_i(\lambda, \mu)$ these constants. This gives

$$\mathcal{N}_0^{\lambda,\mu} := \sum_{i=1}^{k} c_i(\lambda,\mu) v_i \neq 0, \text{ and } G = \lambda p + \mu q \text{ divides } \mathcal{N}_0^{\lambda,\mu}.$$

Indeed, v_i are linearly independent, and furthermore if $G(x,y) = 0$ then $\mathcal{N}_0^{\lambda,\mu}(x,y) = \mathcal{N}_0(x,y) = 0$. Thus, there exists $c \in \mathbb{Q}$ such that $c.G = \mathcal{N}_0^{\lambda,\mu}$. As by construction, $\mathcal{N}_0^{\lambda,\mu} \in \mathbb{C}[X,Y]_{\leq N,0}$, we deduce that G belongs to $\mathbb{C}[X,Y]_{\leq N,0}$ and this contradicts $G(0,0) \neq 0$. Thus we obtain $\mathcal{E}_{N,0}(D) \neq 0$.

Second, we prove that $F = \lambda_0 p + \mu_0 q$ divides $\mathcal{E}_{N,0}(D)$.
F is a Darboux polynomial and belongs to $\mathbb{C}[X,Y]_{\leq N,0}$. Since $\mathcal{E}_{N,0}(D)$ is independent of the chosen basis (with the same arguments used in Proposition 17), we can choose a basis where $v_1 = F$. Then as in Proposition 18 we deduce that F is a factor of $\mathcal{E}_{N,0}(D)$ and this concludes the proof. □

5.2. **Computation of a rational first integral.** Thanks to Proposition 28, we can describe an algorithm which computes a rational first integral.

We denote by (x_k, y_k), $k = 1, \dots, N^6$, the points in $S \times S$ where $S = \{0, \dots, N^3 - 1\}$ and by D_k the following derivation:

$$D_k = A(X + x_k, Y + y_k)\partial_X + B(X + x_k, Y + y_k)\partial_Y.$$

Let $g \in \mathbb{Q}[X,Y]$ with degree smaller than d, $\mathcal{L}_{k,g}$ is the following linear map:

$$\begin{array}{rcl} \mathcal{L}_{k,g} : \mathbb{Q}[X,Y]_{\leq N} & \longrightarrow & \mathbb{Q}[X,Y]_{\leq N+d-1} \\ f & \longmapsto & D_k(f) - g.f \end{array}$$

Lemma 29. *Suppose that D_k has a rational first integral p/q of degree N. We denote by g the cofactor of p and q.*
Then $\dim_{\mathbb{Q}} \ker \mathcal{L}_{k,g} = 2$ and if we denote by $\{\tilde{p}, \tilde{q}\}$ a basis of $\ker \mathcal{L}_{k,g}$ then $\tilde{p}/\tilde{q}$ is a rational first integral of D_k.

Proof. This proof follows very closely the first part of the proof of Theorem 6 in [MO04].
If $f \in \ker \mathcal{L}_{k,g}$ then by Darboux's theorem, see Theorem 5, there exist α and β in $\mathbb{Q}$ such that $f = \alpha p + \beta q$ or f has degree less than N and divides $\alpha p + \beta q$. The last case implies that $(\alpha, \beta) \in \sigma(p,q)$. We deduce that:

$$\ker \mathcal{L}_{k,g} = Span(p,q) \cup Span(f_1) \cup \cdots \cup Span(f_m), \tag{5.2}$$

where f_i is a factor of $\alpha p + \beta q$, $(\alpha, \beta) \in \sigma(p,q)$, and the cofactor of f_i is equal to g. Remark that this union is finite because $\sigma(p,q)$ is finite.
As $\mathbb{Q}$ is infinite, equality (5.2) implies $\ker \mathcal{L}_{k,g} = Span(p,q)$. □

Algorithm Rat-First-Int
Input: A polynomial derivation $D = A(X,Y)\partial_X + B(X,Y)\partial_Y$, and N an integer.
Output: A rational first integral with degree smaller than N or "There exists no rational first integral with degree smaller than N".

(1) Compute $\mathcal{E}_N(D)$.
(2) If $\mathcal{E}_N(D) \neq 0$ then Return "There exists no rational first integral with degree smaller than N", else go to step 3, end If.
(3) Compute the smallest integer n such that $\mathcal{E}_n(D) = 0$ and $\mathcal{E}_{n-1}(D) \neq 0$.
(4) Set F:=0; k:=1;
(5) While $F = 0$ do
  (a) Compute $\mathcal{E}_{n,0}(D_k)$.
  (b) Compute all the irreducible factors $f_1, \ldots, f_m$ of $\mathcal{E}_{n,0}(D_k)$ with degree equal to n.
  (c) For all i:=1, ..., m do: If $\gcd\left(f_i, D_k(f_i)\right) = f_i$ then set $F := f_i$ and go to step 6, end If; end For.
  (d) $k := k + 1$;
  end While.
(6) Compute the cofactor $g := D_{k-1}(F)/F$.
(7) Compute a basis $\{p, q\}$ of $\ker \mathcal{L}_{k-1,g}$.
(8) Return $p/q(X - x_{k-1}, Y - y_{k-1})$.

Proposition 30. *The algorithm Rat-First-Int terminates and uses the While loop at most N^6 times. Furthermore the algorithm Rat-First-Int is correct.*

Proof. The algorithm terminates. We just have to show that the While loop terminates.
In Step 5, thanks to Proposition 20, D has a reduced rational first integral p/q of degree $n \leq N$. Then D_k has a rational first integral $p_k/q_k(X,Y) = p/q(X+x_k, Y+y_k)$ of degree $n \leq N$.

Furthermore p/q is non-composite (thus p_k/q_k is also non-composite). Indeed, if p/q is composite then $p/q = u \circ h$ with $\deg h < n$. This gives

$$0 = D(p/q) = D(u \circ h) = u'(h)D(h),$$

and $u'(h) \neq 0$ because $\deg u \geq 2$. Therefore $D(h) = 0$ and h is a rational first integral with degree smaller than n. Thus by Proposition 20, $\mathcal{E}_{\deg h}(D) = 0$, this contradicts the minimality of n. We deduce then: p/q is non-composite.

Now, remark that the algorithm terminates if the following two conditions are satisfied:

$$p(x_k, y_k) \neq 0 \text{ or } q(x_k, y_k) \neq 0, \tag{5.3}$$

and

$$\big(-q(x_k, y_k) : p(x_k, y_k)\big) \notin \sigma(p_k, q_k) = \sigma(p, q). \tag{5.4}$$

Indeed, in this situation we can apply Proposition 28 and we deduce that there exists a polynomial $F = -q(x_k, y_k)p_k(X, Y) + p(x_k, y_k)q_k(X, Y)$ absolutely irreducible such that $gcd\big(F, D_k(F)\big) = F$.

Now we show that there exists a point (x_k, y_k) in $\{0, \dots, N^3 - 1\}^2$ such that (5.3) and (5.4) are satisfied.
By Bezout's Theorem we just have to avoid N^2 points to satisfy (5.3).
Now, we consider the polynomial

$$\mathcal{P}(X, Y) = \prod_{(\lambda:\mu)\in\sigma(p,q)} \big(\lambda p(X, Y) + \mu q(X, Y)\big).$$

We remark that if $\mathcal{P}(x_k, y_k) \neq 0$ then (5.4) is satisfied. Furthermore, by Proposition 12, $\deg \mathcal{P} \leq N(N^2 - 1)$. Zippel-Schartz's lemma, see [vzGG03, Lemma 6.44], implies that $\mathcal{P}$ has at most $N^6 - N^5$ roots in $\{0, \dots, N^3 - 1\}^2$. Then the algorithm terminates and uses the While loop at most $N^6 - N^5 + N^2 + 1$ times.

The algorithm is correct. If f_i satisfies $\gcd\big(f_i, D_k(f_i)\big) = f_i$ then f_i is a Darboux polynomial. Then by Darboux's theorem, see Proposition 5, we deduce that $f_i = \alpha p_k + \beta q_k$ because $\deg p_k/q_k = n = \deg f_i$.
As p_k/q_k is a first integral, the cofactors of p_k and q_k are equal. Then, we deduce that the cofactors of p_k, q_k and f_i are equal. This cofactor is the polynomial g. Then thanks to Lemma 29 we conclude that the algorithm is correct. □

Now we can prove Theorem 2.

Proof. Thanks to Proposition 30, we just have to prove that the algorithm Rat-First-Int works with $\mathcal{O}\Big(\big(dN \log(\mathcal{H})\big)^{\mathcal{O}(1)}\Big)$ binary operations.
We have already mention that we can compute determinants and solve linear systems in polynomial-time. Thus we can perform Step 1, Step 2 and Step 3 with $\mathcal{O}\Big(\big(dN \log(\mathcal{H})\big)^{\mathcal{O}(1)}\Big)$ binary operations.
Now, we study the While loop.
We recall here that we can shift the variable of a polynomial in polynomial-time see e.g. [BP94, Problem 2.6]. We can also perform linear algebra, compute gcd and divide polynomials in polynomial-time, see e.g. [vzGG03]. Furthermore, as in Corollary 24 we can show that the bit-size of $\mathcal{E}_{N,0}(D)$ belongs to $\mathcal{O}\Big(\big(dN \log(\mathcal{H})\big)^{\mathcal{O}(1)}\Big)$.

Then we can factorize $\mathcal{E}_{N,0}(D)$ with $\mathcal{O}\Big(\big(dN\log(\mathcal{H})\big)^{\mathcal{O}(1)}\Big)$ binary operations. As we use the While loop at most N^6 times we obtain the desired result. □

6. Open questions

6.1. **Liouvillian first integrals.** In this paper we have shown how to compute efficiently Darboux polynomials. Thus this improves the complexity of Prelle-Singer's method. Now the question is: Can we compute efficiently an integrating factor corresponding to a Liouvillian first integral?
In [DDdMS02, DDdM02a, DDdM02b] the authors give an algorithm to compute such integrating factors. The key point is the computation of exponential factors. The definition of an exponential factor is the following:

Definition 31. Given $f, g \in \mathbb{C}[X,Y]$, we say that $e = \exp(g/f)$ is an exponential factor of the derivation D if $D(e)/e$ is a polynomial of degree at most $d-1$.

In [CLP07] the authors define the integrable multiplicity and the algebraic multiplicity.

Definition 32. We say that a Darboux polynomial f has *integrable multiplicity* m with respect to a derivation D, if m is the largest integer for which the following is true: there are $m-1$ exponential factors $\exp(g_j/f^j)$, $j = 1,\dots,m-1$, with $\deg g_j \le j.\deg f$, such that each g_j is not a multiple of f.
We say that a Darboux polynomial f of degree N has *algebraic multiplicity* m with respect to a derivation D, if m is the greatest positive integer such that the mth power of f divides $\mathcal{E}_N(D)$.

C. Christopher, J. LLibre and J.V. Pereira in [CLP07] show that these multiplicities are equal when we consider absolutely irreducible Darboux polynomials. This is a deep result, but unfortunately nowadays there is no simple characterization of exponential factor $\exp(g/f)$ when f is reducible. If we can characterize exponential factors with the ecstatic curve then perhaps we will compute efficiently an integrating factor corresponding to a Liouvillian first integral.

6.2. **Inverse integrating factor.** An inverse integrating factor is a Darboux polynomial with cofactor $\operatorname{div}(A,B)$. An inverse integrating factor R has the following interesting property: The algebraic limit cycles of the polynomial vector field corresponding to D are factors of R, see e.g. [GLV96]. For other results we can read e.g. [CGGL03]. We remark easily that:

$$\begin{aligned} R \text{ is an inverse integrating factor} &\iff \partial_X\Big(\frac{A}{R}\Big) = \partial_Y\Big(\frac{B}{R}\Big) \\ &\iff A\partial_X R + B\partial_Y R = \operatorname{div}(A,B)R. \end{aligned} \tag{6.1}$$

For a given integer N we can compute, if it exists, R with $\deg R \le N$. Indeed, we just have to solve the linear system (6.1). With this strategy and with classical tools of linear algebra we can compute R with $\mathcal{O}(N^6)$ arithmetic operations if $N \ge d$.

This kind of linear system also appears when we study absolute factorization, see [Rup86, Rup99, Gao03, CL07, Sch07]. Indeed, we can compute the absolute factorization of a given polynomial R with a solution (A,B) of (6.1).

In [CL07] the authors use this kind of linear system and show that the absolute factorization of R can be performed with $\tilde{\mathcal{O}}(N^4)$ arithmetic operations. We recall that "soft Oh" is used for readability in order to hide logarithmic factors in cost estimates. Then the question is the following:
Can we perform the computation of an inverse integrating factor in a deterministic way with $\tilde{\mathcal{O}}(N^4)$ arithmetic operations instead of $\mathcal{O}(N^6)$?

7. Acknowledgment

I thank L. Busé, G. Lecerf, J. Moulin-Ollagnier, and J.-A. Weil for their encouragements during the preparation of this work.

References

[AHS03] S. Abhyankar, W. Heinzer, and A. Sathaye. Translates of polynomials. In *A tribute to C. S. Seshadri (Chennai, 2002)*, Trends Math., pages 51–124. Birkhäuser, Basel, 2003.

[AKS07] M. Avendaño, T. Krick, and M. Sombra. Factoring bivariate sparse (lacunary) polynomials. *J. Complexity*, 23:193–216, 2007.

[Aut91] L. Autonne. Sur la théorie des équations différentielles du premier ordre et du premier degré. *Journal de l'École Polytechnique*, 61:35–122, 1891.

[BC08] L. Busé and G. Chèze. On the total order of reducibility of a pencil of algebraic plane curves. Preprint, 2008.

[BCS97] P. Bürgisser, M. Clausen, and M. Shokrollahi. *Algebraic Complexity Theory*, volume 315 of *(Grundlehren der mathematischen Wissenschaften)*. Springer, 1997.

[Ber70] E. R. Berlekamp. Factoring polynomials over large finite fields. *Math. Comp.*, 24:713–735, 1970.

[BLS+04] A. Bostan, G. Lecerf, B. Salvy, É. Schost, and B. Wiebelt. Complexity Issues in Bivariate Polynomial Factorization. In *Proceedings of ISSAC 2004*, pages 42–49. ACM, 2004.

[Bod08] A. Bodin. Reducibility of rational functions in several variables. *Israel J. Math.*, 164:333–347, 2008.

[BP94] D. Bini and V. Pan. *Polynomial and matrix computations. Vol. 1*. Progress in Theoretical Computer Science. Birkhäuser Boston Inc., Boston, MA, 1994. Fundamental algorithms.

[BvHKS09] K. Belabas, M. van Hoeij, J. Klüners, and A. Steel. Factoring polynomials over global fields. *J. Th. Nombres Bordeaux*, 21:15–39, 2009.

[CG03] J. Chavarriga and M. Grau. Some open problems related to 16b Hilbert problem. *Sci. Ser. A Math. Sci. (N.S.)*, 9:1–26, 2003.

[CGGL03] J. Chavarriga, H. Giacomini, J. Giné, and J. Llibre. Darboux integrability and the inverse integrating factor. *J. Differential Equations*, 194(1):116–139, 2003.

[Chr94] C. Christopher. Invariant algebraic curves and conditions for a centre. *Proc. Roy. Soc. Edinburgh Sect. A*, 124(6):1209–1229, 1994.

[Chr99] C. Christopher. Liouvillian first integrals of second order polynomial differential equations. *Electron. J. Differential Equations*, pages No. 49, 7 pp. (electronic), 1999.

[CL07] G. Chèze and G. Lecerf. Lifting and recombination techniques for absolute factorization. *J. Complexity*, 23(3):380–420, 2007.

[CLP07] C. Christopher, J. Llibre, and J. Vitório Pereira. Multiplicity of invariant algebraic curves in polynomial vector fields. *Pacific J. Math.*, 229(1):63–117, 2007.

[CMS06] S. C. Coutinho and L. Menasché Schechter. Algebraic solutions of holomorphic foliations: an algorithmic approach. *J. Symbolic Comput.*, 41(5):603–618, 2006.

[CMS09] S. C. Coutinho and L. Menasché Schechter. Algebraic solutions of plane vector fields. *J. Pure Appl. Algebra*, 213(1):144–153, 2009.

[Dar78] G. Darboux. Memoire sur les équations diff'érentielles du premier ordre et du premier degré. *Bull. Sci. Math.*, 32:60–96, 123–144, 151–200, 1878.

[DDdM02a] L. G. S. Duarte, S. E. S. Duarte, and L. A. C. P. da Mota. Analysing the structure of the integrating factors for first-order ordinary differential equations with Liouvillian functions in the solution. *J. Phys. A*, 35(4):1001–1006, 2002.

[DDdM02b] L. G. S. Duarte, S. E. S. Duarte, and L. A. C. P. da Mota. A method to tackle first-order ordinary differential equations with Liouvillian functions in the solution. *J. Phys. A*, 35(17):3899–3910, 2002.

[DDdMS02] L. G. S. Duarte, S. E. S. Duarte, L. A. C. P. da Mota, and J. E. F. Skea. An extension of the Prelle-Singer method and a Maple implementation. *Comput. Phys. Comm.*, 144(1):46–62, 2002.

[DLA06] F. Dumortier, J. Llibre, and J. C. Artés. *Qualitative theory of planar differential systems*. Universitext. Springer-Verlag, Berlin, 2006.

[DLS98] V. A. Dobrovol'skii, N.V. Lokot', and J.-M. Strelcyn. Mikhail Nikolaevich Lagutinskii (1871–1915): un mathématicien méconnu. *Historia Math.*, 25(3):245–264, 1998.

[DT89] R. Dvornicich and C. Traverso. Newton symmetric functions and the arithmetic of algebraically closed fields. In *Applied algebra, algebraic algorithms and error-correcting codes (Menorca, 1987)*, volume 356 of *Lecture Notes in Comput. Sci.*, pages 216–224. Springer, Berlin, 1989.

[FG10] A. Ferragut and H. Giacomini. A new algorithm for finding rational first integrals of polynomial vector fields. to appear in Qualitative Theory of Dynamical Systems, 2010.

[Gao03] S. Gao. Factoring multivariate polynomials via partial differential equations. *Math. Comp.*, 72(242):801–822 (electronic), 2003.

[Gin07] J. Giné. On some open problems in planar differential systems and Hilbert's 16th problem. *Chaos Solitons Fractals*, 31(5):1118–1134, 2007.

[GLV96] H. Giacomini, J. Llibre, and M. Viano. On the nonexistence, existence and uniqueness of limit cycles. *Nonlinearity*, 9(2):501–516, 1996.

[Gor01] A. Goriely. *Integrability and nonintegrability of dynamical systems*, volume 19 of *Advanced Series in Nonlinear Dynamics*. World Scientific Publishing Co. Inc., River Edge, NJ, 2001.

[Hew91] C. G. Hewitt. Algebraic invariant curves in cosmological dynamical systems and exact solutions. *Gen. Relativity Gravitation*, 23(12):1363–1383, 1991.

[HS75] E. Horowitz and S. Sahni. On computing the exact determinant of matrices with polynomial entries. *J. ACM*, 22(1):38–50, 1975.

[Jou79] J.-P. Jouanolou. *Équations de Pfaff algébriques*, volume 708 of *Lecture Notes in Mathematics*. Springer, Berlin, 1979.

[Kal85a] E. Kaltofen. Fast parallel absolute irreducibility testing. *J. Symbolic Comput.*, 1(1):57–67, 1985.

[Kal85b] E. Kaltofen. Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization. *SIAM J. Comput.*, 14(2):469–489, 1985.

[Kal90] E. Kaltofen. Polynomial factorization 1982–1986. In *Computers in mathematics (Stanford, CA, 1986)*, volume 125 of *Lecture Notes in Pure and Appl. Math.*, pages 285–309. Dekker, New York, 1990.

[Kal92] E. Kaltofen. Polynomial factorization 1987-1991. In I. Simon, editor, *Proc. LATIN '92*, volume 583, pages 294–313. Springer-Verlag, 1992.

[KLL88] R. Kannan, A. K. Lenstra, and L. Lovász. Polynomial factorization and nonrandomness of bits of algebraic and some transcendental numbers. *Math. Comp.*, 50(181):235–250, 1988.

[Lec06] G. Lecerf. Sharp precision in Hensel lifting for bivariate polynomial factorization. *Math. Comp.*, 75(254):921–933 (electronic), 2006.

[Len84] A. K. Lenstra. Factoring multivariate integral polynomials. *Th. Comp. Science*, 34:207–213, 1984.

[LLL82] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.

[Lor93] D. Lorenzini. Reducibility of polynomials in two variables. *J. Algebra*, 156(1):65–75, 1993.

[LV08] J. Llibre and C. Valls. Darboux integrability and algebraic invariant surfaces for the Rikitake system. *J. Math. Phys.*, 49(3):032702, 17, 2008.

[LZ00] J. Llibre and X. Zhang. Invariant algebraic surfaces of the Rikitake system. *J. Phys. A*, 33(42):7613–7635, 2000.

[Man93] Y.-K. Man. Computing closed form solutions of first order ODEs using the Prelle-Singer procedure. *J. Symbolic Comput.*, 16(5):423–443, 1993.

[MM97] Y.-K Man and M. A. H. MacCallum. A rational approach to the Prelle-Singer algorithm. *J. Symbolic Comput.*, 24(1):31–43, 1997.

[MO04] J. Moulin Ollagnier. Algebraic closure of a rational function. *Qual. Theory Dyn. Syst.*, 5(2):285–300, 2004.

[Pai91] P. Painlevé. Mémoire sur les équations différentielles du premier ordre. *Annales Scientifiques de l'École Normale Supérieure*, 8:9–59, 103–140, 201–226, 276–284, 1891.

[Per01] J.V. Pereira. Vector fields, invariant varieties and linear systems. *Ann. Inst. Fourier (Grenoble)*, 51(5):1385–1405, 2001.

[Poi91] H. Poincaré. Sur l'intégration algébrique des équations différentielles du premier ordre et du premier degré. *Rend. Circ. Mat. Palermo*, 5:161–191, 1891.

[PS83] M. J. Prelle and M. F. Singer. Elementary first integrals of differential equations. *Trans. Amer. Math. Soc.*, 279(1):215–229, 1983.

[Rup86] W.M. Ruppert. Reduzibilität Ebener Kurven. *J. Reine Angew. Math.*, 369:167–191, 1986.

[Rup99] W.M. Ruppert. Reducibility of polynomials $f(x, y)$ modulo p. *J. Number Theory*, 77(1):62–70, 1999.

[Sch84] A. Schönhage. Factorization of univariate integer polynomials by Diophantine approximation and an improved basis reduction algorithm. In *Automata, languages and programming (Antwerp, 1984)*, volume 172 of *Lecture Notes in Comput. Sci.*, pages 436–447. Springer, Berlin, 1984.

[Sch00] A. Schinzel. *Polynomials with special regard to reducibility*, volume 77 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2000. With an appendix by Umberto Zannier.

[Sch07] P. Scheiblechner. On the complexity of deciding connectedness and computing Betti numbers of a complex algebraic variety. *J. Complexity*, 23(3):359–379, 2007.

[Sin92] M.F. Singer. Liouvillian first integrals of differential equations. *Trans. Amer. Math. Soc.*, 333(2):673–688, 1992.

[Tra85] B. Trager. *On the integration of algebraic functions*. PhD thesis, M.I.T., 1985.

[Val05] C. Valls. Rikitake system: analytic and Darbouxian integrals. *Proc. Roy. Soc. Edinburgh Sect. A*, 135(6):1309–1326, 2005.

[Vis93] A. Vistoli. The number of reducible hypersurfaces in a pencil. *Invent. Math.*, 112(2):247–262, 1993.

[vzGG03] J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, Cambridge, second edition, 2003.

[Wei] M. Weimann. A lifting and recombination algorithm for rational factorization of sparse polynomials. *J. Complexity*, to appear.

[Yap00] C.K. Yap. *Fundamental problems of algorithmic algebra*. Oxford University Press, Inc., New York, NY, USA, 2000.

Institut de Mathématiques de Toulouse, Université Paul Sabatier Toulouse 3, MIP Bât 1R3, 31 062 TOULOUSE cedex 9, France

E-mail address: guillaume.cheze@math.univ-toulouse.fr